УДК 681.3;004.056.53

В.К. Фисенко, Е.П. Максимович, О.В. Мелех
Государственное научное учреждение «Объединенный институт проблем информатики» Национальной академии наук Беларуси, г. Минск
fisenko@ nevman.bas-net.by

Система лингвистических показателей и критериев принятия решений при аттестации систем защиты информации

Предложены структура Программы аттестации систем защиты информации информационных систем, а также лингвистические показатели и критерии принятия решений на этапах предварительного ознакомления с информационной системой, в том числе с системой защиты информации, исследования информационной системы, оценки качества документации к системе защиты информации и проверки соответствия представляемой документации требованиям нормативных правовых актов, в том числе технических нормативных правовых актов.

Введение

Под аттестацией согласно [1], [2] понимается комплекс организационно-технических мероприятий, в результате которых соответствие системы защиты информации (СЗИ) требованиям нормативных правовых актов в области защиты информации, в том числе технических правовых актов, подтверждается и оформляется аттестатом соответствия.

Аттестация СЗИ информационных систем (ИС), по существу, только начинает внедряться в практику Республики Беларусь. В связи с этим целесообразно для решения этих проблем использовать не только национальные нормативные и правовые документы, но и накопленный опыт мирового сообщества [3-8].

Особенностью аттестации СЗИ является то обстоятельство, что она проводится специализированной организацией по заявке владельца защищенной ИС и, как правило, в районе ее размещения. В таких условиях использовать при решении задач аттестации математические модели, основанные на количественных значениях показателей и критериев принятия решений, затруднительно. Эти трудности обусловлены достаточно широким классом подлежащих решению задач аттестации. Нельзя не учитывать и то обстоятельство, что различные ИС оснащаются СЗИ, обладающими различными уровнями информационной безопасности, что, естественно, требует разработки не одного, а нескольких математических методов и моделей для каждого типового класса ИС. Очевидно, что по мере накопления практического опыта аттестации СЗИ будут разработаны специальные методики, использующие количественные значения показателей и критериев принятия решений, однако пока в Беларуси такие методики не разработаны.

Целью настоящей работы является представление научной общественности и практикам в области аттестации СЗИ системы лингвистических показателей и критериев принятия решений, использование которых обеспечивает решение наиболее существенных задач, определенных процедурой аттестации СЗИ.

Предлагаемый подход базируется на документах «Положение о порядке аттестации систем защиты информации» и «Общая методология испытания продуктов и систем информационных технологий» (ИСО/МЭК18045: 2005 года) на соответствие Заданиям по безопасности, разработанным по требованиям определенного уровня гарантии оценки (УГО).

1 Цели и задачи аттестации

Целью аттестации является проверка соответствия СЗИ ИС требованиям действующего законодательства в области информационной безопасности, а также нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов, и выдача на этой основе аттестата соответствия.

Для достижения указанной цели должны быть решены следующие задачи:

– анализ исходных данных по аттестуемой СЗИ ИС;

– предварительное ознакомление с СЗИ ИС;

– анализ разработанной документации по защите информации в СЗИ ИС на соответствие требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов;

– обследования СЗИ ИС;

– проведение испытаний средств защиты информации и оценка СЗИ ИС в реальных условиях ее функционирования;

– анализ результатов испытаний средств защиты информации и СЗИ ИС и принятие решения о выдаче аттестата соответствия;

– выдача аттестата соответствия (при положительных результатах испытаний).

Перечисленные задачи определяют основу Программы аттестации СЗИ ИС, а результаты решения перечисленных задач характеризуют степень эффективности СЗИ и защищенности ИС.

Рассмотрим порядок решения наиболее значимых из перечисленных задач.

2 Предварительное ознакомление с информационной системой

Предварительное ознакомление с СЗИ рассматривается как один из ключевых этапов аттестации. Порядок предварительного ознакомления с ИС и СЗИ основан на участии специалистов специализированной организации в следующих мероприятиях:

– заслушивание владельца СЗИ ИС по всем вопросам, затрагивающим функционирование ИС;

– демонстрация работоспособности ИС, практическая проверка реализации уровня защиты, в том числе функций защиты операционной системы и антивирусных программ.

После предварительного ознакомления с ИС и ее СЗИ эксперты должны решить следующие задачи:

1. Оценить текущее, в том числе программное, состояние ИС.

Текущее состояние ИС является удовлетворительным, если ее назначение и архитектура соответствуют требованиям, предъявляемым к разработке данной ИС, а информация, обрабатываемая в системе, является точной, достоверной и оперативной.

Программное состояние ИС является удовлетворительным, если оно выполняет все функции, возлагаемые на данную ИС, и соответствует всем принципам обеспечения безопасности программного обеспечения (ПО), включающим в себя:

– ограничение доступа к эталонам программных средств, недопущение неавторизованного их изменения;

– профилактическое выборочное тестирование и полное сканирование программных средств на наличие преднамеренных дефектов;

– идентификацию ПО на момент ввода его в эксплуатацию в соответствии с предполагаемыми угрозами безопасности ПО и его контроль;

– обеспечение модификации программных изделий во время их эксплуатации путем замены отдельных модулей без изменения общей структуры и связей с другими модулями;

– строгий учет и каталогизация всех сопровождаемых программных средств, а также собираемой, обрабатываемой и хранимой информации;

– статистический анализ информации о всех процессах, рабочих операциях, отступлениях от режимов штатного функционирования ПО;

– гибкое применение дополнительных средств защиты ПО в случае выявления новых, непрогнозируемых угроз информационной безопасности.

2. Уяснить и оценить организацию управления и мониторинга ИС.

Управление ИС базируется на использовании текущих сведений о состоянии системы, с тем чтобы воздействовать на ИС с целью достижения заданных целей. Для управления может использоваться интерактивная система поддержки принятия решений, реализованная в рамках исследуемой ИС.

Мониторинг ИС состоит в непрерывном наблюдении за ее состоянием и регистрации событий в реальном времени. Для этого могут использоваться показания приборов и сведения, получаемые в результате обмена информацией, поисковых запросов и др.

3. Оценить порядок настройки политики безопасности на серверах и рабочих станциях.

Политика безопасности на серверах и рабочих станциях под управлением ОС семейства MS Windows реализуется с помощью мастера настройки безопасности.

Основными подходами к обеспечению безопасности компьютеров являются: обеспечение физической безопасности компьютеров, выключение ненужных сервисов, настройка параметров ОС (для этого обычно используются шаблоны безопасности), установка обновлений и пакетов обновлений.

4. Оценить состояние антивирусной защиты серверов и рабочих станций.

5. Оценить состояние организации обмена данными в рамках информационной системы.

6. Оценить организацию хранения данных у владельца системы.

Хранение данных нуждается в технологиях, отличных от технологий защиты передаваемых данных. Технологии, используемые для защиты хранимых данных, делятся на несколько категорий: контроль доступа, шифрование данных, мониторинг, защита от разрушения хранимых данных, резервное копирование данных и восстановление после катастроф.

7. Определить наличие и оценить содержание правил и инструкций пользователей для работы в сети, стандарты и политики безопасности.

Организация функционирования СЗИ ИС обеспечивается на основе стандарта ISO 17799, стандарта ISO 15408, отражающего требования по обеспечению безопасности систем, содержащих программные средства.

Политика безопасности определяет стратегию и тактику построения СЗИ и является основой для разработки целого ряда документов безопасности: руководств, процедур, практик, должностных инструкций и пр., позволяющих выполнить требования нормативно-правовых документов.

При работе с сетью разрабатываются два вида инструкций:

– должностные инструкции администратора сетей, описывающих круг обязанностей администратора для данного предприятия. Это может быть не только обеспечение бесперебойной работы самой сети, но и обеспечение сетевой безопасности (защиты от несанкционированного доступа в сеть, просмотра или изменения системных файлов и данных), а также безопасности межсетевого взаимодействия. В должностную инструкцию могут входить все вопросы, касающиеся написания инструкций по работе с сетевым ПО пользователей и доведения их до пользователей услугами сети;

– правила и инструкции пользователей для работы в сети, описывающие правила и инструкции по работе, а также ответственность за нарушения данных правил.

После предварительного ознакомления с ИС и СЗИ и установления положительной оценки их качества по всем вышеприведенным показателям осуществляется более детальное ознакомление с системой и с документами на систему.

3 Обследование системы защиты информации информационной системы

Основной целью информационного обследования СЗИ ИС является определение текущего фактического состояния уровня обеспечения защиты информации и его соответствие предъявленным требованиям безопасности.

Обследование ИС и СЗИ основывается на результатах анализа и оценки исходных данных (документации) по ИС и аттестуемой СЗИ. Основными задачами информационного обследования СЗИ ИС являются:

– проверка соответствия представленных заявителем исходных данных реальным условиям размещения, установки (монтажа) и эксплуатации аттестуемой СЗИ ИС;

– проверка технологического процесса обработки и хранения защищаемой информации, анализ информационных потоков, проверка использованных для обработки защищаемой информации программно-технических средств и систем;

– проверка состояния организации работ и выполнения организационно-технических требований по защите информации;

– оценка уровня подготовки кадров и распределения ответственности за выполнение требований по обеспечению защиты информации.

Для проведения обследования СЗИ ИС в качестве исходных данных владельцем СЗИ ИС должен предоставляться определенный список документов и сведений, подлежащих исследованию. Анализ соответствия реального состояния ИС и ее СЗИ исходным данным (декларируемому уровню) проводится с использованием следующих показателей и критериев принятия решений.

Показатель: полнота описания СЗИ ИС.

Критерий: Документация на СЗИ ИС обладает полнотой описания, если количество и наименование ее характеристик (атрибутов, свойств, функций, параметров и т.д.) полностью соответствует количеству и наименованию характеристик (атрибутов, свойств, параметров, процедур и т.д.) описываемой СЗИ ИС в исходных данных (документации), представленных Владельцем.

Обязательным условием для принятия решения о полноте является представление информации по форме и содержанию в соответствии с требованиями нормативных правовых актов, в том числе технических нормативных актов, проектной и (или) эксплуатационной документации, организационно-распорядительной документации.

Показатель: адекватность отображения.

Критерий: Характеристики СЗИ ИС должны в полной мере соответствовать конкретным характеристикам описываемой СЗИ ИС в исходных данных (документации), представленных владельцем.

Показатель: достаточность уровня детализации.

Критерий: Уровень детализации информации в исходных данных (документации), представленных владельцем СЗИ ИС, является достаточным в следующих случаях:

– информация содержит минимальный, но достаточный набор положений для описания характеристик (атрибутов, свойств, функций, параметров и т.д.) СЗИ ИС;

– информация обоснована (доказательно или путем ссылки) принятыми в исходных данных (документации) положениями или доказательствами;

– представленная в исходных данных (документации) информация не является, по мнению эксперта, избыточной, что может привести к ошибкам в принятии пользователем решений.

Процесс обследования СЗИ ИС включает в себя проведение следующих проверок:

– *Организационной структуры СЗИ ИС.*

Критерий принятия решения: Если реальная структура, перечень и описание функций подсистем операционной системы соответствуют описанной в исходных данных (документации) организационной структуре СЗИ ИС по критериям полноты описания, адекватности отображения, достаточности уровня детализации, – то эксперт делает вывод о положительном результате проверки организационной структуры СЗИ ИС.

– *Состава и структуры комплекса технических средств и программного обеспечения СЗИ ИС.*

Критерий принятия решения: Если в результате инвентаризации перечень и структура, условия размещения, установки (монтажа) и эксплуатации комплекса технических средств (ТС) и ПО соответствуют исходным данным (проектной и эксплуатационной документации) по критериям полноты описания, адекватности отображения, достаточности уровня детализации, то эксперт делает вывод о положительном результате проверки состава и структуры комплекса ТС и ПО СЗИ ИС.

– *Технологического процесса обработки и хранения защищаемой информации, анализ информационных потоков ИС.*

Критерий принятия решения: Если перечень и характеристики обнаруженных информационных потоков (входящих, исходящих и циркулирующих внутри), технологического процесса (режимов) обработки и хранения защищаемой информации в ИС соответствуют исходным данным (документации) по критериям полноты описания, адекватности отображения, достаточности уровня детализации, то эксперт делает вывод о положительном результате проверки технологического процесса обработки и хранения защищаемой информации, информационных потоков в ИС.

– *Применения программно-технических средств и СЗИ ИС для обработки защищаемой информации.*

Критерий принятия решения: Если применение и значения параметров конфигурации программно-технических средств и систем полностью соответствуют (отсутствуют ошибки и неучтенные параметры конфигурации) исходным данным (проектной и эксплуатационной документации) по критериям полноты описания, адекватности отображения, достаточности уровня детализации, то эксперт делает вывод о положительном результате проверки применения программно-технических средств и СЗИ ИС для обработки защищаемой информации.

– *Выполнения организационно-технических требований.*

Критерий принятия решения: Если реально принимаемые меры по выполнению организационно-технических требований (например, порядок и процедуры обращения с защищаемой информацией, порядок применения СЗИ, в том числе уровень подготовки кадров и распределение ответственности за организацию и обеспечение защиты информации и т.д.) соответствуют исходным данным (организационно-распорядительным документам) по критериям полноты описания, адекватности отображения, достаточности уровня детализации, то эксперт делает вывод о положительном результате проверки выполнения организационно-технических требований.

На заключительном этапе обследования ИС делается заключение об уровне ее защищенности. Для определения уровня защищенности ИС предлагается выделять три уровня защиты: базовый, расширенный и усиленный.

ИС имеет *базовый уровень защиты*, если в ней реализована система защиты, обладающая следующими функциональными характеристиками:

– спецификация включает только встроенные средства защиты ОС типа WINDOWS 2003, WINDOWS XP, WINDOWS VISTA и др.;

– параметры областей безопасности ОС настроены на функциональные требования безопасности, представленные в задании по безопасности СЗИ ИС;

– гарантийные требования безопасности соответствуют уровню гарантии, определенному в задании по безопасности СЗИ ИС;

– ИС обеспечена сертифицированными антивирусными программными средствами.

Базовый уровень защиты рекомендован для реализации в ИС, не имеющих выхода в другие системы.

ИС имеет *расширенный уровень защиты*, если в ней реализована система защиты, обладающая следующими функциональными характеристиками:

– в ИС реализован базовый уровень защиты;

– спецификация дополнена межсетевым экраном, средствами обнаружения атак.

Расширенный уровень защиты рекомендуется для реализации в ИС, не имеющих выхода в глобальные вычислительные сети типа Интернет.

ИС имеет *усиленный уровень защиты*, если в ней реализована система защиты, обладающая следующими функциональными характеристиками:

– в ИС реализован расширенный уровень защиты;

– спецификация дополнена специальными средствами безопасности, разработанными с учетом специфики ИС, в том числе средствами криптографической защиты, электронной цифровой подписью и др.

Усиленный уровень защиты рекомендуется для реализации в СЗИ ИС, имеющих выход в глобальные вычислительные сети типа Интернет. Гарантии безопасности, соответствующие усиленному уровню защиты, предусматривают методическое проектирование, тестирование, углубленную проверку и т.д. По результатам проведенного обследования представляются технический отчет, содержащий результаты обследования ИС и СЗИ, и акт обследования ИС и СЗИ.

4 Анализ данных по аттестуемой системе защиты информации

Анализ исходных данных производится с использованием следующих показателей качества: соответствие исходных данных (нормативным документам); полнота исходных данных; репрезентативность исходных данных; неизбыточность исходных данных; достоверность реального состояния безопасности; уровень детализации исходных данных; охват всех существенных показателей безопасности; связность и внутренняя непротиворечивость данных, приведенных как в пределах одного, так и различных документов.

Приняты следующие критерии принятия решений по приведенным выше показателям качества.

Критерий соответствия исходных данных.

Представленные владельцем ИС исходные данные по наименованию и содержанию соответствуют перечню данных по СЗИ, определенных нормативными документами. Обязательным условием для принятия решения о соответствии является предоставление информации по форме и содержанию в соответствии с требованием действующих нормативных документов.

Критерий полноты исходных данных.

Исходные данные представлены в объеме, достаточном для проведения аттестации с требованием действующих нормативных документов.

Критерий репрезентативности исходных данных.

Репрезентативность данных связана с правильностью их отбора и формирования.

Критерий неизбыточности исходных данных.

Представленные владельцем ИС исходные данные не содержат сведений, не относящихся к безопасности и запутывающих, затрудняющих процесс аттестации.

Критерий адекватности отображения.

Представленный владельцем ИС документ, входящий в перечень исходных данных и содержащий конкретные характеристики аттестуемой СЗИ ИС, в полной мере соответствует характеристикам реальной СЗИ ИС. Все сведения изложены ясно, непредвзято и не вводят в заблуждение потенциальных пользователей, не допускают неоднозначной трактовки и неопределенности.

При предоставлении данных должна быть закреплена ответственность лиц, предоставивших информацию, подтверждены их опыт и компетентность.

Критерий достаточности уровня детализации.

Уровень детализации представленной в документе информации является достаточным лишь в следующих случаях:

– представленная в документе информация содержит минимальный, но достаточный набор показателей для принятия опытным экспертом правильного решения относительно качества, целевого назначения и реализуемости представленных положений;

– изложенная в документе информация определяет все основные концептуальные положения, на базе которых сформулированы основные функциональные положения документа;

– все основные положения, принятые в документе, четко обоснованы либо имеется ссылка на ранее реализованное положение, программу или устройство;

– представленная в документе детализация не является, по мнению эксперта, избыточной.

Критерий охвата всех показателей безопасности.

Представленная в документе информация должна отражать степень реализации всех или отдельных требований безопасности, связанных с обеспечением конфиденциальности, целостности и доступности активов ИС.

Критерий связности и внутренней непротиворечивости.

Представленная в документе информация должна удовлетворять свойствам связности и непротиворечивости. Связность трактуется как свойство, определяющее зависимости между различными элементами (частями, структурами) предмета, объекта, процесса или текста, а непротиворечивость – как логический критерий корректности (правильности, согласованности) некоторого утверждения, доказательства, рассуждения или их совокупности.

При анализе связности и непротиворечивости исходных данных целесообразно принять во внимание следующую конкретизацию этих понятий на уровне общих текстообразующих категорий научно-технического текста.

Связность – категория единства тематического содержания текста, характеризующая степень взаимосвязи частей текста и направленности на решение определенной общей задачи, требующая наличия причинно-следственных отношений, строгой логической последовательности изложения и представления информации (каждый последующий элемент вытекает из предыдущего или является следующим звеном в повествовании или рассуждении). Различают локальную связность (связность текста в пределах раздела) и глобальную (связь между разделами, обеспечивающую единство текста как смыслового целого). При оценке по показателю связности целесообразно принять во внимание родственную ей категорию цельности – четко выраженную смысловую замкнутость текста, представление информации в виде законченного целого.

Непротиворечивость – категория корректности (правильности, согласованности) представления информации. Различают локальную непротиворечивость (непротиворечивость информации на уровне разделов) и глобальную (согласованность между разделами документа).

Для каждого из указанных выше типов анализируемых данных приведенные общие критерии могут быть дополнены и конкретизированы с учетом их специфики.

5 Анализ документации на соответствие требованиям нормативных правовых актов, в том числе технических нормативных правовых актов

К действующим нормативно-правовым актам Республики Беларусь, регулирующим отношения в сфере информационной безопасности, на сегодняшний день относятся:

1) нормативные правовые акты в области защиты информации (Конституция, законодательство в области информационной безопасности, постановления Совета Министров, Министерства труда и социальной защиты и др.);

2) нормативные технические акты в области защиты информации (технические регламенты, государственные и международные стандарты);

3) документация к СЗИ, используемая при ее аттестации (задание по безопасности, исходные данные по УГО1 – УГО4, конструкторская и программная документация).

Перечисленные первые две группы документов должны соответствовать требованиям нормативных правовых актов, в том числе технических правовых актов, по следующим показателям: оценка соответствия, форма подтверждения соответствия, схема подтверждения соответствия.

Под оценкой соответствия понимается деятельность эксперта по определению представленных документов требованиям указанных актов, определенных в Национальной системе подтверждения соответствия в области технического нормирования и стандартизации.

Под формой подтверждения соответствия понимается установленный порядок документального удостоверения соответствия разработанных документов требованиям нормативных правовых и технических правовых актов.

Под схемой (порядком) подтверждения понимается установленная последовательность действий, результаты которых рассматриваются в качестве доказательства соответствия разработанных документов требованиям нормативных правовых и технических правовых актов.

При анализе документов, применяемых при испытаниях СЗИ (документы третьей группы), используются специальные показатели. Предложен следующий порядок подтверждения соответствия применительно к разрабатываемым документам в области защиты информации.

Каждый документ третьей группы используется в качестве исходных данных при проведении испытаний системы. Порядок их использования описан в конкретных методиках испытаний для определенного уровня гарантии. В качестве показателей оценки соответствия используются показатели полноты, связности и непротиворечивости. Существо этих показателей заключается в следующем:

Полнота – категория достаточности представленной в документе информации в соответствии с требованиями, определенными нормативными или правовыми документами; достаточность выразительных или дедуктивных средств для представления необходимой информации в документе.

Связность определяет импликативную связь вида «если…, то…» между представленными документами.

Непротиворечивость определяет согласованность, отсутствие противоречий между документами, относящихся к конкретной реализации СЗИ.

Если по совместному решению экспертной комиссии и владельца ИС метод испытаний в качестве доказательства соответствия не применяется, в этом случае работы по подтверждению соответствия проводятся в следующем порядке.

Каждый документ проверяется:

– на степень соответствия правовому акту – указывается конкретный нормативный документ;

– на степень удовлетворения требования полноты: если документ содержит весь перечень разделов, подразделов в соответствии с требованиями правовых актов (стандартов), то, значит, документ удовлетворяет требованиям полноты;

– на степень соответствия представленных в документах перечня средств безопасности и мер гарантии спецификации, приведенной в задании по безопасности.

В случае выявления несоответствия заявленных показателей (характеристик) обязательным требованиям нормативных правовых актов в сфере технической защиты информации рассмотрение заявки на проведение экспертизы продукции приостанавливается с извещением об этом заявителя. Рассмотрение заявки на проведение экспертизы продукции возобновляется только после устранения заявителем указанных недостатков.

Заключение

Краткое ознакомление с лингвистическими показателями и критериями принятия решений при аттестации систем защиты информации информационных систем показывает, что их перечень достаточно значительный по количеству. В процессе приобретения опыта аттестации этот перечень показателей и критериев принятия решений будет уточнен и более конкретизирован.

Литература

1. Положение о порядке аттестации систем защиты информации. Постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 675.
2. Об информации, информатизации и защите информации. Закон Республики Беларусь от 10.11.2008.
3. Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений / Заде Л. – М. : Мир, 1976. – 165 с.
4. Модели принятия решений на основе лингвистической переменной / А.Н. Борисов [и др]. – Рига : Зинатне,1982. – 256 с.
5. О сертификации продукции и услуг. Закон Российской Федерации от 10.061993 № 5151-1.
6. Положение по аттестации объектов информатизации по требованиям безопасности информации. – Государственная техническая комиссия России, 1994.
7. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. – Государственная техническая комиссия России, 1994.
8. Аттестационные испытания АС по требованиям безопасности информации. Типовая методика испытаний объектов информатизации по требованиям безопасности информации. – Государственная техническая комиссия России, 1995.

В.К. Фісенко, О.П. Максімовіч, О.В. Мелех

Система лінгвістичних показників та критеріїв прийняття рішень при атестації систем захисту інформації

Запропоновані структура Програми атестації систем захисту даних інформаційних систем, а також лінгвістичні показники та критерії прийняття рішень на етапах попереднього ознайомлення з інформаційною системою, у тому числі з системою захисту інформації, дослідження інформаційної системи, оцінки якості документації до системи захисту інформації та перевірки відповідності документації, що представлена, вимогам нормативних правових актів, у тому числі технічних правових актів.

V.K. Fisenko, E.P. Maksimovich, O.V. Melekh

The System of Linguistic Indicators and Decision Making Criteria for Certification of Information Security Systems (ISS)

The framework of information protection system information systems certification Program is proposed. The linguistic indexes and decision criteria on the stage of information systems previewing, including its information protection systems, the stage of information systems study, the stage of information protection system documentation quality evaluation and the stage of conferred documentation compliance with normative legislative acts requirements, including technical ones, checking are suggested

Статья поступила в редакцию 13.07.2010.